Özmen Emre DEMİRKOL (demirkol@uekae.tubitak.gov.tr) 04.04.2005

SNORT-2.3, ACID FEDORA 3 – PF, SNORTSAM OPENBSD 3.6

AÇIKLAMA

Bu belge yeni versiyon snort(2.3) için Fedora 3 üzerinde yapılması gereken ayarları, ACID, snortsam pluginin eklenmesi ve bununla ilgili ayarları ve pf ile entegrasyonu için yapılması gerekenleri anlatmaktadır.

Bu belgenin hazırlanmasındaki amaç, daha önce yazılan dökümanların 2.2 ve daha eskiler için olması ve 2.3 için yetersiz kalmasındandır. Aynı zamanda tamamen serbert bir firewall-ids çözümünün anlatılması amacı güdülmüştür.

SNORT ve ACID KURULUMU

Öncelikle FC3 olan bir makinenizin olduğunu ve bunun üzerinde Apache, MySQL ve PHP'nin kurulu olduğunu varsayıyorum. Tabi bunlarin updatelerini de yapmayı unutmayın :))

Ayrıca eğer sisteminizde kurulu değilse, pcre, pcre-devel ve libpcap'in rpmlerini http://rpm.pbone.net adresinden veya kendi bildiğiniz bir siteden indirerek siteminize ekleyiniz.

Daha sonra http://www.snort.org/dl/binaries/linux/ adresinden;

- snort-2.3.2-0.fdr.1.i386.rpm
- snort-mysql2.3.2-0.fdr.1.i386.rpm

http://acidlab.sourceforge.net/ adresinden;

- acid-0.9.6b23.tar.gz

http://www.aditus.nu/jpgraph/jpdownload.php adresinden;

- jpgraph-1.17.tar.gz

http://adodb.sourceforge.net/#download adresinden;

- adodb461.tgz

dosyalarını indiriniz.

İlk olarak;

```
rpm -ivh snort-2.3.2-0.fdr.1.i386.rpm
rpm -ivh snort-mysql-2.3.2-0.fdr.1.i386.rpm
```

komutlariyla snort ve snort-mysql'i sisteme kurunuz.

MySQL'inizi henüz şifrelendirmediyseniz;

```
# mysqladmin -u root -p password yeni_sifreniz  <- [Enter]
# Enter password:  <-[Enter]
```

şeklinde şifrenizi değiştiriniz. Arkasından snort için bir veritabanı ve kullanıcı oluşturup, haklar tanumlamanız gerekmektedir. Bunun için;

```
# mysql -u root -p <-[Enter]
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('password_from_snort.conf');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

işlemlerini sırasıyla takip ediniz.

Sıra Snort veritabanının tablolarını sisteme eklemeye geldi. Burada yaşanılacak sıkıntı, Snort'un veritabanı tablolarını içeren sql dosyasının rpmlerin içinden çıkmamasıdır. Bu nedenle http://www.snort.org/dl/current/snort-2.3.2.tar.gz adresinden kaynak dosyayı indirmelisiniz.

- tar -xzvf snort-2.3.2.tar.gz

şeklinde dosyayı açın ve

```
# mysql –u snort -p < ~snort-2.3.2/schemas/create_mysql snort <-[Enter]
Enter Password: snort_şifreniz <-[Enter]
```

şeklinde veritabanı tablolarını sisteme ekleyin. Arkasından yapmanız gereken;

```
# vi /etc/snort/snort.conf
```

kullanarak

```
var HOME_NET any -> var HOME_NET [sizin_ip_klasınız / subnetiniz]
output database: log, mysql, user=snort password=snort dbname=snort host=localhost
```

bölümlerini kendinize göre düzenlemektir.

Daha sonra

```
# mv acid-0.9.6b23.tar.gz /var/www/html/
# mv jpgraph-1.17.tar.gz /var/www/
# mv adodb461.tgz /var/www/
```

işlemlerini yapınız ve

```
# cd /var/www/html
# tar -xzvf acid-0.9.6b23.tar.gz
# mv acid-0.9.6b23 acid
# chown apache.apache
```

```
# cd ../
# tar -xzvf  jpgraph-1.17.tar.gz
# mv  pgraph-1.17  jpgraph
# chown apache.apache
# tar -xzvf  adodb461.tgz
# mv adodb461 adodb
# chown apache.apache
```

şeklinde klasörleri açıp, hakları belirleyiniz.

Bunda sonra sıra */var/www/html/acid/acid_conf.php* dosyasına girip gerekli ayarlamaları yapmanız gerekmektedir. Sırasıyla ;

```
$DBlib_path = "/var/www/adodb";

$alert_dbname   = "snort_db_adi";
$alert_host     = "snort_db_sunucusu";
$alert_port     = "";
$alert_user     = "snort_db_kullanicisi";
$alert_password = "snort_db_sifresi";

$archive_dbname   = "snort_db_adi";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "snort_db_kulanicisi";
$archive_password = "snort_db_sifresi";

$ChartLib_path = "/var/www/jpgraph/src";
```

satırlarını düzenleyiniz. Artık servisleri çalıştırabilirsiniz.

```
# /etc/init.d/snort start
# /etc/init.d/httpd start
```

Şimdi sunucunuza *http://localhost/acid* adresinden ACID'i ilk kez çalıştırıp, veritabanına kendisini eklemesini sağlamalısınız. Bu açılan ilk ekranda *Setup_Page* i klikleyin. Daha sonra karşınıza gelen yeni ekranda *Create_ACID_AG* butonuna basıp tabloların oluşmasını sağlayın. Eğer hiçbir sorun çıkmadıysa, ana sayfaya dönüp ACID'i kullanmaya başlayabilirsiniz.

Önemli Not = Eğer */etc/sysconfig/snort* dosyasında ALERTMODE u kapatmazsanız, ACID logları okuyamaz.

ALERTMODE=fast -> #ALERTMODE=fast

OpenBSD ÜZERİNDE PF, SNORTSAM ve SNORT ile ENTEGRASYONU

Bu bölümde elinizde hazır bir OpenBSD olduğunu düşünerek diğer işlemlere geçiyorum. Eğer isterseniz http://www.openbsd.org/faq/faq4.html adresinden OpenBSD kurulumuna bakabilirsiniz.

OpenBSD üzerinde *pf*'i açılışta çalışır hale getirmek ve OpenBSD üzerindeki ethernetlerini birbirine forward ettirmek için aşağıdaki işlemleri yapınız.

```
# vi /etc/rc.conf
pf=NO -> pf=YES

# vi /etc/sysctl.conf
net.inet.ip.forwarding=0 -> net.inet.ip.forwarding=1

# vi /etc/pf.conf
pass in all
pass out all
```

Burada verilen pf kuralları giriş-çıkış yapan bütün paketlere izin verir. Siz kendi sisteminize uygun kuralları belirleyip *pf.conf* içine yazmalısınız. PF ile ilgili olarak *http://www.openbsd.org/faq/pf* adresine bakabilirsiniz.

Şimdi sırasıyla Fedora Core 3 makineniz için ;

http://www.snortsam.net/files/snort-2.3-plugin/compiled/linux/snort-2.3-mysql-sam.tar.gz

OpenBSD makineniz için;

cvs -d :pserver:anonymous@cvs.snortsam.net:/cvsroot co snortsam

veya

wget ftp://ftp.snortsam.net/public/snortsam/snortsam-v2_multi-threaded/snortsam-src-2.31.tar.gz

komutuyla snortsam paketini indiriniz.

Snortsam'i kurmak, ayarlamak ve çalıstırmak için sırayla su işlemleri yapınız (OpenBSD üzerinde);

```
# cd snortsam
# sh makesnortsam.sh
# cp snortsam /usr/bin/          (binary dosyayi kopyalayin)
# cp snortsam.conf.sample /etc/snortsam.conf
# echo "/usr/bin/snortsam /etc/snortsam.conf  &" >> /etc/rc.local
```

Aşağıdaki satırları */etc/snortsam.conf* dosyasına ekleyiniz.

accept *snort_sunucusu_ip_adresi/netmask*, *snortsam_sifreniz*
pf anchor=fwsam auto=1 log=1 eth=*ethernet_adı* table=blockedipsINOUT

Eğer isterseniz log turması için;

logfile /var/log/snortsam.log

satırını da ekleyebilirsiniz.

Önemli Not = snortsam.conf içine yazılan "pf" ayarları ile ilgili açıklamayı http://www.snortsam.net/files/snortsam-v2_multi-threaded/docs/README.pf adresinden bulabilirsiniz.

Snortsam'i ilk kez çalıştırmak için OpenBSD'nizi reboot edebilir veya *"/usr/bin/snortsam /etc/snortsam.conf &"* kumutunu çalıştırabilirsiniz.

Şimdi snort'u snortsam ile konuşabilmesi için ayarlamalısınız. Bunun için FEDORA'nızda daha önceden indirdiğiniz *snort-2.3-mysql-sam.tar.gz* dosyasını

```
# tar -xzvf  snort-2.3-mysql-sam.tar.gz
```

şeklinde açıp içinden çıkan snort dosyasına(binary) sırasıyla aşağıdaki işlemleri uygulayınız.

```
# rm -rf  /usr/local/bin/snort
# cp snort /usr/local/bin/
```

Önemli Not = Yeni snort dosyası çalışırken *mysql.sock* dosyasını */tmp* altında aradığından, snort'u çalıştırdığınızda çalışmış gibi görünür ama çalışmaz ve */var/log/messages* dosyasında aşağıdaki gibi bir hata alırsınız.

FATAL ERROR: database: mysql_error: Can't connect to local MySQL server through socket '/tmp/mysql.sock'

Bu hatayı düzeltmek için */etc/init.d/snortd* içinde şu değişiklikleri yapmalısınız.

```
case "$1" in
  start)
      echo -n "Starting snort: "

-----

case "$1" in
  start)
      ln -s /var/lib/mysql/mysql.sock /tmp/mysql.sock
      echo -n "Starting snort: "
```

```
stop)
        echo -n "Stopping snort: "
        killproc snort
        rm -f /var/lock/subsys/snort
        echo
```

```
stop)
        echo -n "Stopping snort: "
        killproc snort
        rm -f /var/lock/subsys/snort
        rm -f /tmp/mysql.sock
        echo
```

Bundan sonra yapmanız gereken son ekleme */etc/snort/snort.conf* içinde ve şu şekildedir;

output alert_fwsam: *snortsam_sunusu_ip_adresi/snortsam_sifreniz*

Artık yapmanız gereken son şey snort'u yeniden çalıştırmaktır.

BLOKLAMA TESTİ

/etc/snort/rules/local.rules dosyası içine aşağıdaki örnek kuralları yazın. Bu kuralların ilkine göre, 55550 numaralı porttan gelen bağlantılarda sadece log işlemi yaparken 55555 numaralı porttan gelen isteklerde istek yapan ipnin geliş yönünde 5 dakika sürelye bağlantısını kesecektir.

```
alert tcp any any -> sizin_ip 55550 (msg:"TEST log 55550/tcp";  sid:5555550;)
alert tcp any any -> sizin_ip 55555 (msg:"TEST block 55555/tcp";  sid:5555555; fwsam:src[in],5min;)
```

Kurallar Snort'un kural dosyaları içindeki satırların sonuna *fwsam:kim[nasıl],zaman* şeklinde eklenir.

kim = Snort kuralına bağlı olarak bloklanacak ip -> src(kaynak) , dst(hedef)

nasıl = Bloklanacak ipnin hangi yönde iletişiminin kesileceği bilgisi -> in , out , src , dst , either(her iki yönde – ön tanımlı olan budur) , this(bu bağlantı için) v.b.

zaman = Blok süresi -> seconds(saniyeler), minutes(dakikalar) , hours(saatler) , days(günler) , weeks(haftalar) , months(aylar) , years(yıllar).
PER , INF , ALWAYS ise kalıcı blok içindir.

Örnekler = fwsam: src[either],15min – fwsam:dst[out],1 days 5 hours – fwsam:src, 1 hours

Eğer *nasıl* için birşey belirtmezseniz her iki yöne doğru kabul edilir. Zaman için birşey belirtmezseniz 5 dakika kabul edilir.

Yukarıda yazdığımız örnek kuralları denemek için telnet yoluyla hedef ipye kuralda belirlenen portlardan bağlanmayı deneyin. İlk kural için olan porta bağlandığınızda *pf* tarafında log dosyasında veya sistemde sadece uyarı logu göreceksiniz. Fakat ikinci kural için belirlenen porta bağlandığınızda bağlanmaya çalışan ip adresi Snortsam tarafından *pf*'e bloklatılacaktır.

Aşağıdaki komutları kullanarak bloklanmış ip adreslerini görebilirsiniz.

pfctl -a fwsam -t blockin -Ts -> Gelen yöndeki bloklu ip adresleri
pfctl -a fwsam -t blockinout -Ts -> Her iki yönde bloklu ip adresleri
pfctl -a fwsam -t blockout -Ts -> Giden yöndeki bloklu ip adresleri

GÜLE GÜLE KULLANIN...